UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,917	06/26/2003	Kyung-Hun Jang	784-51 (SI-19122-US)	8113

66547 7590 01/30/2008

THE FARRELL LAW FIRM, P.C.
333 EARLE OVINGTON BOULEVARD
SUITE 701
UNIONDALE, NY 11553

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
01/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/607,917	JANG ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending in this office action.

2. Applicant's arguments, filed November 27, 2007, have been fully considered but they are not persuasive.

Specification

3. The amendment filed May 24, 2007, is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: page 9, line 26, applicant canceled "carrier waves" from the original disclosure. Amending the specification was not required in response to the 101 rejection, amending the claim language was required; applicant has amended the claim as required. Applicant is required to cancel the new matter (by re-adding the canceled language) in the reply to this Office Action.

Claim Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claim 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (U.S. Patent No. 7,221,764) in view of Watanabe et al. (U.S. Patent No. 7,072,657).

Regarding claims 1, 8, 11, and 12, Cohen et al. teaches a roaming method/computer readable **storage** medium/apparatus for a wireless station using a plurality of encryption keys allocated according to a plurality of access authorization classes, said method comprising the steps of:

- When a wireless station requests said access point to perform initial authentication differentiating said plurality of encryption keys according to a plurality of access authorization types and said wireless station obtaining in advance an encryption key set including the differentiated plurality of encryption keys for respective access points (fig. 2C, fig. 3 and col. 5, lines 5-25);
- Receiving a command to communicate with an access point not available for communication using an encryption key currently selected in the encryption key set (col. 8, line 64 through col. 9, line 11);
- Determining an access authorization to the access point not available for communications (col. 5, lines 5-9);
- Selecting an encryption key from the encryption key set obtained in advance corresponding to the determined access authorization (col. 5, lines 10-18); and

- Using the selected encryption key to encrypt a transmission message and communicate with the access point not available for communication (col. 5, lines 18-21).

Cohen et al. does not teach setting an access authorization to an access point in advance.

Watanabe et al. teaches setting an access authorization to an access point in advance (fig. 7, ref. num 502).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine setting an access authorization to an access point in advance, as taught by Watanabe et al., with the method of Cohen et al. It would have been obvious for such modifications because a handoff arrangement is necessary to have seamless communications. Setting access authorization in advance helps ensure a fast handoff because there is no delay waiting for authorization to take place.

Regarding claims 2, 9, and 13, Cohen et al. as modified by Watanabe et al. teaches wherein the access authorization types include:

- A class 1 that indicates access authorization to an access point to which the wireless station is assigned;

- A class 2 that indicates access authorization to predetermined access points included in a local area network (LAN) to which the wireless station is assigned;
- A class 3 that indicates access authorization to all access points included in the LAN to which the wireless station is assigned; and
- A class 4 that indicates access authorization to multiple access points included in a wide area network (WAN) (see fig. 4, ref. num 408A-D, 410A-B, and 412A-F of Watanabe et al.).

Regarding claim 3, Cohen et al. as modified by Watanabe et al. teaches further comprising a step of a wireless station desiring to communicate with an access point selecting from the plurality of encryption keys an encryption key corresponding to the access authorization to the access point and communicates data with the access point, wherein the wireless station has a plurality of encryption keys corresponding to access authorization types (see col. 7, lines 17-40 of Watanabe et al.).

Regarding claims 4 and 10, Cohen et al. as modified by Watanabe et al. teaches wherein differentiating encryption keys step further comprises:

- Determining access authorization to an access point when the access point is requested to perform initial authentication by said wireless station (see fig. 7, ref. num 502 of Watanabe et al.);

- Obtaining an encryption key and generating a shared key set including the obtained encryption keys in accordance with the determination result of the first step (see col. 6, line 57 through col. 7, line 16 of Watanabe et al.);
- Determining access authorization to an access point belonging to an LAN by a LAN authentication server which is requested to perform initial authentication by the wireless station (see fig. 7, ref. num 510 of Watanabe et al.);
- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the third step (see col. 7, lines 41-64 of Watanabe et al.);
- Determining access authorization to an access point belonging to a WAN by a WAN authentication server which is requested to perform initial authentication by the wireless station (see fig. 7, ref. num 516 of Watanabe et al.); and
- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the fifth step (see col. 7, lines 41-64 of Watanabe et al.).

Regarding claim 5, Cohen et al. as modified by Watanabe et al. teaches wherein the first step further comprises a step of the wireless station requesting an access point to perform authentication, and the access point which is requested to perform authentication determining whether or not access authorization to the access point corresponds to a class 1, said class 1 indicating access authorization to an access point to which the wireless station is assigned (see col. 7, lines 17-40 of Watanabe et al.).

Regarding claim 6, Cohen et al. as modified by Watanabe et al. teaches wherein the third step of claim 4 further comprises the steps of:

- The LAN authentication server determining whether or not the access authorization to the access point corresponds to a class 2, said class 2 indicating access authorization to predetermined access points included in a LAN to which the wireless station belongs to;
- If a determination result indicates that the access authorization corresponds to said class 2, obtaining an encryption key of class 2, and determining whether or not the access authorization corresponds to a class 3, said class 3 indicating access authorization to all access points included in the LAN to which the wireless station belongs to; and
- If a determination result indicates that the access authorization corresponds to said class 3, obtaining an encryption key of class 3 (see fig. 4, ref. num 408A-D, 410A-B, and 412A-F of Watanabe et al.).

Regarding claim 7, Cohen et al. as modified by Watanabe et al. teaches all the limitations of claims 4 and 6, above. However, Cohen et al. as modified by Watanabe et al. does not specifically teach wherein the second step of claim 6 further comprises the steps of: allocating a null encryption key if the determination result of the first step indicates that the access authorization does not correspond to said class 2; determining whether the access authorization corresponds to class 3; and allocating a null

encryption key if a determination result indicates that the access authorization does not correspond to class 3.

Official Notice is taken that a null encryption key is allocated if the determining steps determines that the access authorization does not correspond to class 2 or 3.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine allocating a null encryption key based on a determination that the access authorization does not correspond to class 2 or 3, with the method of Cohen et al./Watanabe et al. It would have been obvious for such modifications because a null encryption key ensures that access is not obtained when access authorizations do not match. When a mobile device does not have authorization for a certain class, a null encryption key will prevent further access. If the null encryption key was not allocated to the mobile device, other data would be allocated and could possibly allow authorization.

Claim 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda et al. (U.S. Patent No. 6,289,102) in view of Watanabe et al. (U.S. Patent No. 7,072,657).

Regarding claim 14, Ueda et al. teaches a computer readable **storage** medium storing instructions which, when executed causes execution of a program implementing

a structure of a wireless data packet in a wireless network that comprises a wireless station and an access point, the structure comprising:

- A header of said data packet transmitted through the wireless network (fig. 1, SECTOR HEADER FIELD);
- An encrypted data field in which data contents to be transmitted are encrypted and stored (fig. 1, USER DATA FIELD and fig. 13, section E); and
- An error correction field, which is used to correct data error (fig. 1, ECC).

Ueda et al. does not teach an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point, **the access authorization information being used for allocating encryption keys according to access authorization classes**.

Watanabe teaches an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point, **the access authorization information being used for allocating encryption keys according to access authorization classes** (fig. 4, ref. num 408A-D, 410A-B, and 412A-F and col. 5, line 8-49).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a field for access authorization information storing, as taught by Watanabe et al., with the medium of Ueda et al. It would have been obvious

for such modifications because the access authorization field tells the device being accessed which level of access needs to take place (see col. 5, lines 50-67 of Watanabe et al.).

Regarding claim 15, Ueda et al. as modified by Watanabe et al. teaches wherein the access authorization types include:

- A class 1 that indicates access authorization to an access point to which the wireless station is assigned;
- A class 2 that indicates access authorization to predetermined access points included in a local area network (LAN) to which the wireless station is assigned;
- A class 3 that indicates access authorization to all access points included in the LAN to which the wireless station is assigned; and
- A class 4 that indicates access authorization to multiple access points included in a wide area network (WAN) (see fig. 4, ref. num 408A-D, 410A-B, and 412A-F of Watanabe et al.).

Response to Arguments

6. Applicant argues that Cohen does not teach a plurality of access authorization types (page 8).

Regarding applicant arguments, examiner disagrees. Cohen teaches that, depending on the client, either a rolling key is used or a fixed key is used. Each type,

rolling or fixed, acts as an authorization type, with its own set of keys for each (col. 4, lines 30-48 and col. 5, lines 45-61).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/28/08